绿盟工业网络安全监测预警平台

白皮书

【绿盟科技】

■ 文档编号	NSF-TR-RPM-101	■ 密级	完全公开
■ 版本编号		■ 日期	
■ 撰 写 人		■ 批准人	

© 2019 绿盟科技

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属绿盟科技所有，受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 版本变更记录

时间	版本	说明	修改人

目录

一. 工业网络安全管理的新需求和挑战

需求分析

过去，工业系统中物理隔离的方式足以提供良好的防护，如今，这种情况将不复存在，据 SANS 研究所发现，35%的工业网络故障事件由网络攻击引起。

在今年的 RSA 大会上，ICS 和供应链攻击成为最热的议题之一。众所周知，国内工业产业链中 ICS 安全产业起步明显晚于国外的，而近年来以工业环境为目标的恶意攻击出现显著增长。供应链和业务中断的风险在过去三年里一直高居全球企业风险的榜首，而面向生产的网络安全成为能源、制造工业企业首要新兴问题。对于运营工业或关键基础设施的企业，风险日益壮大。

工业安全影响远超过商业和名誉保护。在多数情况下，当涉及到工业系统威胁、攻击、破坏时，往往首要考虑生态、社会和宏观经济因素。因此，工业系统等关键基础设施的关键节点和网络保护需要足够高的防护等级才能对抗日益增长的网络安全威胁。同时，工业环境需要一套的综合的解决方案通过安全预警响应和纵深防御策略提升技术流程的可用性。

随着企业信息化的不断发展，公司信息化资产数量日趋增多、系统的关联性和复杂度不断增强，然而当前信息安全形势日益严峻，工业信息安全防护工作面临前所未有的困难和挑战。为了更好监控和保障信息系统运行，及时识别和防范安全风险，同时满足国家和行业监管要求，保证信息安全管理工作的依法合规，亟需建立一个日志集中管理平台，做到事前预警、事中监控、事后分析，全面提升信息安全管理与防护水平。

同时，工业互联技术及攻防技术的不断演进，企业对信息安全技术人员的依赖日益加深，对技术人员的安全能力也有了更高的要求。这不仅加剧了技术人员的需求缺口，也增加了管理人员使用成本。企业在转变生产方式和业务拓展的大背景下，运维和人员数量和人员成本的与日俱增，又使得企业预算捉襟见肘。

而两化融合、工业 4.0 驱动着制造业、过程控制、基础设施以及其他工业控制系统的连通性，给这些工业控制系统带来的威胁不断上升。

互连设备的引入，IT 和 OT 的整合，给 ICS 系统带来了新的安全挑战。企业希望能够知道在 ICS 中，什么是正常的操作，同时通过正常操作建立基线来判断什么是不正常的、意外的或者潜在的恶意操作。这就需要在工控环境中建立态势感知系统。态势感知是在大规模系

© 2019 绿盟科技

密级：完全公开

统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

专精于工业网络的态势感知系统的四大特征是：

- ✓ IT 和 OT 的深度融合
- ✓ 结合跨行业业务场景的行为基线
- ✓ 可视化的预警与感知

不同行业客户对工控平台有着不同的需求特性。大致分为以下几个方面：

① 针对不同行业的安全场景模型(行为基线建模），工控的业务操作流程进行梳理，形成各个工业操作业务流的健康性监控

② 工业网络的工控场景数据收集、处理和分析

③ 主动防御和安全预警

④ 全面了解工控网络的全局风险，以工控领域常见的拓扑或直观呈现的方式表现网络环境及各设备的运行状态和安全状态

⑤ 需要协助运维人员快速解决故障及事件

⑥ 指导安全工作和决策

⑦ 符合等保及合规要求

面临的挑战

当前主流的工业网络管理系统主要面临着以下几种挑战：

1） 多源异构数据采集需求

随着公司信息安全水平的提升，公司安全防护产品越来越多，安全品牌也也各式各样，同时对于后续的安全分析，已经不仅仅只是安全设备的职责，本次平台建设需要做好多源异构全数据采集规划，对于所有网络内可用的安全分析辅助信息进行收集，包括但不限于安全设备日志、业务系统日志、网络流量等等，为后续平台数据挖掘及关联分析做好数据准备。

2） 工业网络数据存储与分析需求

由于采集数据的多元性、异构性和工业网络性，还会包括对于网络流量的采集，因此平台所采集的数据量将是一个巨大的数字，并且涉及到今后对于数据的挖掘以及关联分析和历史查询分析，存储的时间至少要六个月，因此工业网络数据的存储问题在平台设计之初就应该重点考虑，且为保障平台运转的延续性和对于 APT 等新型攻击的深度挖掘，还要考虑到存储空间不足时数据存储的可扩展能力。

工业网络数据采集后，对于已知攻击的实时分析、历史数据的挖掘分析，以及对工业网络内外网数据、事件、文件等的关联分析、检索、实时在线检测、离线检测，发现

© 2019 绿盟科技

密级：完全公开

高级的 APT 攻击和信息泄漏行为能力要成为平台具备的基本能力，计算能力的强弱直接决定着平台今后的实用性。

3） 安全指标及态势的可视化展现需求

作为大数据安全分析平台，在分析能力基础上应有一个人性化的、简单实用的展示界面，平台分析结果需采用量化指标形式呈现，直观展示当前网络攻击、病毒木马、主机漏洞、终端异常行为等重点安全监控指标，在出现高威胁攻击时可通过实时攻击地图进行展示，同时结合历史数据分析，展示全公司安全态势及发展趋势。

4） 信息安全一体化建设和监管需求

在安全运维工作中，安全运维人员面对不同类型并且部署于不同位置的安全设备，难以在全局上了解全网存在的脆弱性是如何分布的、面临的安全威胁有哪些，也难以判断第一时间应该优先对哪些脆弱性进行修补和控制，对哪些威胁进行诊断和分析。按照设备告警时间的顺序处理威胁告警、控制和修补资产脆弱性，往往会导致运维人员错过真正需要诊断分析的威胁和真正需要控制和修补的漏洞，无法及时有效地降低网络安全风险。

安全设备集中管理工具可以对安全威胁告警及其分类，并帮助安全运维人员识别最需要进行诊断分析的威胁。同样，通过安全设备集中管理工具，安全运维人员才能查看全网资产脆弱性分布情况，从而进一步根据资产重要性和脆弱性的风险级别识别出最需要控制和修补的脆弱性。

5） 如何保障企业业务系统协同管理

无论是传统企业环境中，还是在未来的“云计算”环境中，不可避免的存在一个或者多个业务系统并存的情况。 这些业务系统可能是网管、SOC 、SIEM 或者 CMDB 等。它们自身定位不同，并且负责着不同类型信息的收集、汇总以及展示。如何与这些相关业务系统协同运维，打破各自为战的“信息孤岛”是摆在企业面前的另一道障碍。

6） 如何保障业务平台系统的可用性

业务系统的可用性体现在：对新兴的威胁防御以及资产维度上的威胁感知。传统的工业网络管理系统强调对单个设备和性能的可用性管理，缺乏通过多设备联动，对复杂网络威胁攻击（APT 攻击）的检测和防护。同时，从设备监控视角出发，过渡地强调设备故障的及时诊断，已经不能够从根本上保障核心业务系统的可用性，更缺乏从核心资产维度的监控和分析。

如何应对挑战

© 2019 绿盟科技

密级：完全公开

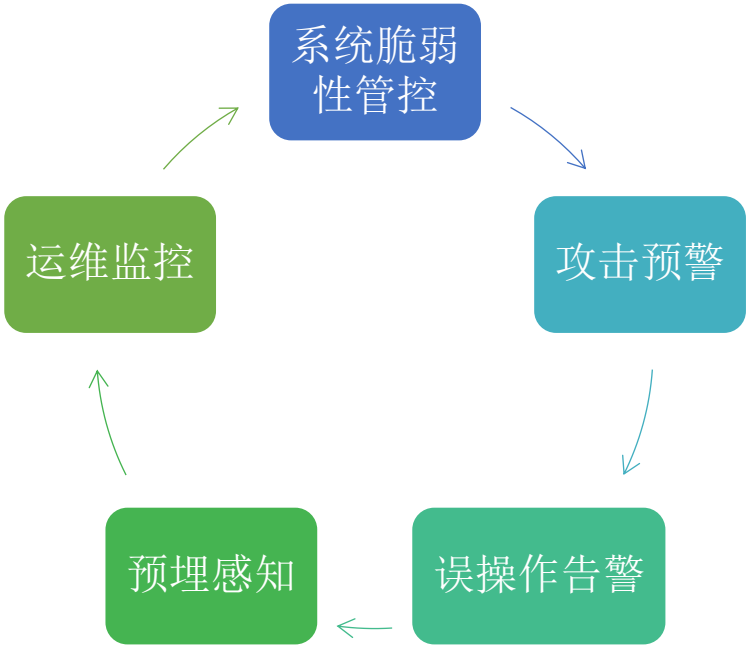
客户需要一套全新的安全管理系统来应对传统网络和工业网络数据带来的所有挑战，该系统能够通过数据采集和大数据分析，利用机器学习等先进技术，协助企业 IT 运维人员和安全分析人员快速发现威胁。以情报为驱动，针对企业工业网络资产情况进行全方位的监控和告警，协助用户进行网络安全威胁的统一管理。同时，这个系统应该是一个开放的平台，能够与客户的其他管理系统实现协同工作。

二. 绿盟工业网络安全监测预警平台

产品概述

绿盟工业网络安全监测预警平台从工业控制系统安全的角度，对工控系统的各类 IT 和 OT 设备数据进行采集，包括业务设备日志采集、安全设备事件收集、网络流量数据采集、安全设备配置采集等功能。平台对采集得到的结果进行统一分析与展示，发现工控网络内部的异常行为，如新增资产、时间异常、新增关系、负载变更、异常访问等行为，实现对工控现场安全事件的预警与响应。

绿盟工业网络安全监测预警平台可以对工业网络中各类上位机服务器、工控终端、网络交换设备、工控安全设备进行集中化的性能状态监控、安全事件的集中展示、安全风险的评估、工控分区分域的健康等级，以及依赖于工控知识库的安全响应与处置。



© 2019 绿盟科技

密级：完全公开

图 2.1 融合业务的安全保障闭环

产品架构

NSFOCUS INSP 主要由数据采集层、数据分析层、系统功能层、可视化展示层共四个部分组成，可以在各种不同场景的工业网络环境中进行灵活的部署和管理,如图所示：

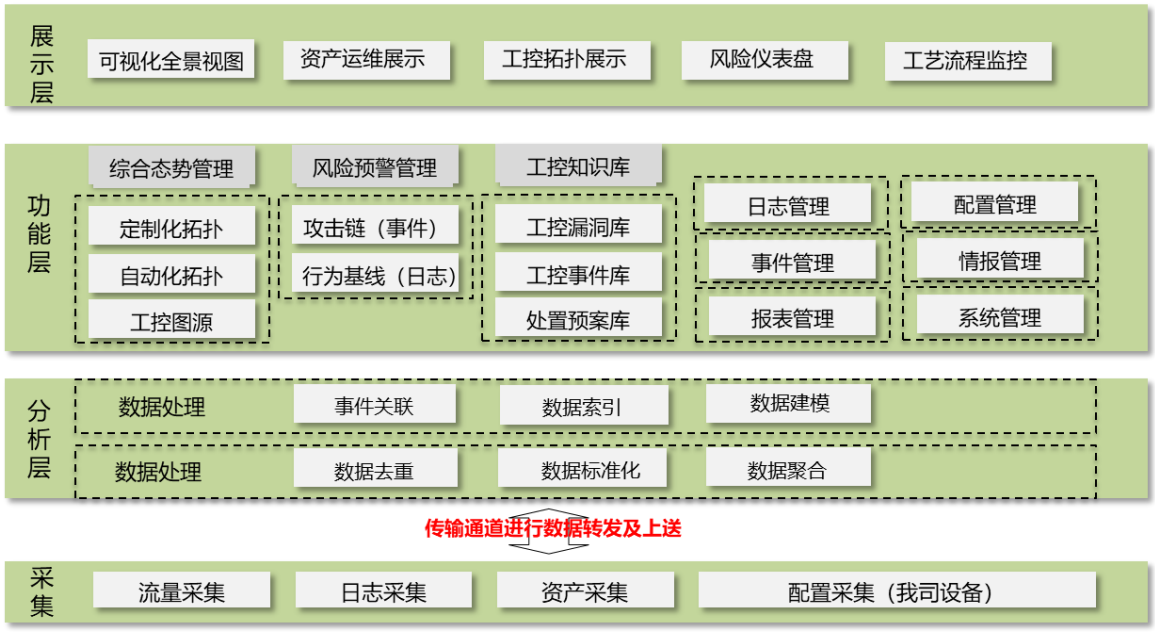


图 2.2 NSFOCUS INSP 系统架构图

① 数据采集层

提供多种数据格式的接口，如 syslog、snmp 等协议格式，收集工业网络中各类上位机服务器、工控终端、网络交换设备、工控安全设备的日志信息和配置信息。

② 数据分析层

对采集后的来自不同类型设备的日志、事件、配置信息进行集中分析和处理。

② 系统功能层

在该层实现系统的应用功能的实现。包括基于工控网络拓扑的综合态势管理、基于攻击链和业务行为基线的风险预警管理、基于工控事件库和处置预案库的工控知识库以及其他核心功能模块。

④ 可视化展示层

在该层实现可视化的交互展示，包括工业网络风险全景视图，资产运维监视视图，工控拓扑图，风险仪表盘等可视化模块。

产品亮点

© 2019 绿盟科技

密级：完全公开

全面的日志集中管理

- 支持 SYSLOG、SNMP Trap、FTP、SFTP、JDBC、ODBC、Net flow 等多种日志采集方式。
- 支持但不限于网络设备，如上位机、工业安全网关、工控安全审计、主机安全卫士、交换机、路由器、入侵检测等，并进行日志关联和量化分析。

PB 级的日志处理能力

- 平台使用 Spark 技术，在并发内存内处理机制方面能够带来数倍于其它采用磁盘访问方式的解决方案，借助离线计算引擎在小时级别内，即可完成对 PB 数量级的数据挖掘。可以为大规模、超大规模网络提供高性能的日志采集，存储和审计功能。例如：6 个月内的安全事件之间的相关性，安全事件之间的影响程度，安全事件之间的规律性等并以报表形式进行输出。

可视化的综合态势管理

工业网络安全监测预警平台可以通过网络拓扑或直观呈现的方式表现网络环境及各设备的运行状态和安全状态，从而达到对工控网络中的各类设备进行集中的状态及性能监控的目的。目前主要通过定制化工控拓扑的方式来实现工控网络综合态势的管理和呈现。呈现在首页的工控网络拓扑可根据工业现场需求进行定制化的拓扑绘制。

同时，针对不同行业工业现场网络架构的特异性，平台内置具有行业特性的工控网络安全监控拓扑，用户可根据自身行业特点选择相应行业的网络拓扑结构，并在其基础上进行组态化的拓扑绘制，使最终呈现的工控网络拓扑符合展示及监控要求。

© 2019 绿盟科技

密级：完全公开

综合态势管理还包括可视化的攻击链状况展示、风险仪表盘展示、告警事件类型分布展示、资产风险分布展示、最新安全事件列表等可视化模块。

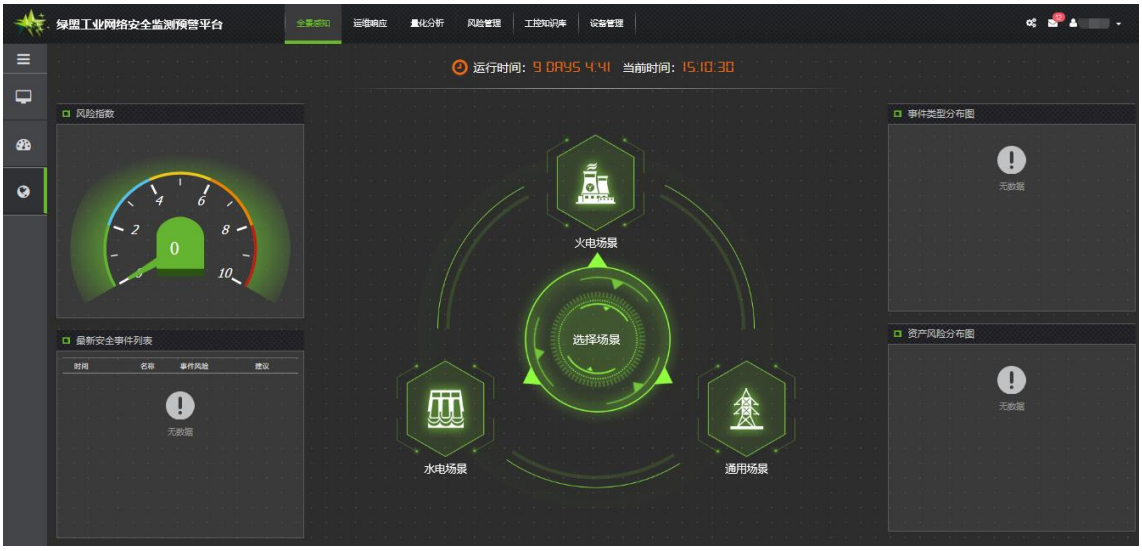


图 2.3 工控网络综合态势管理和场景定制向导

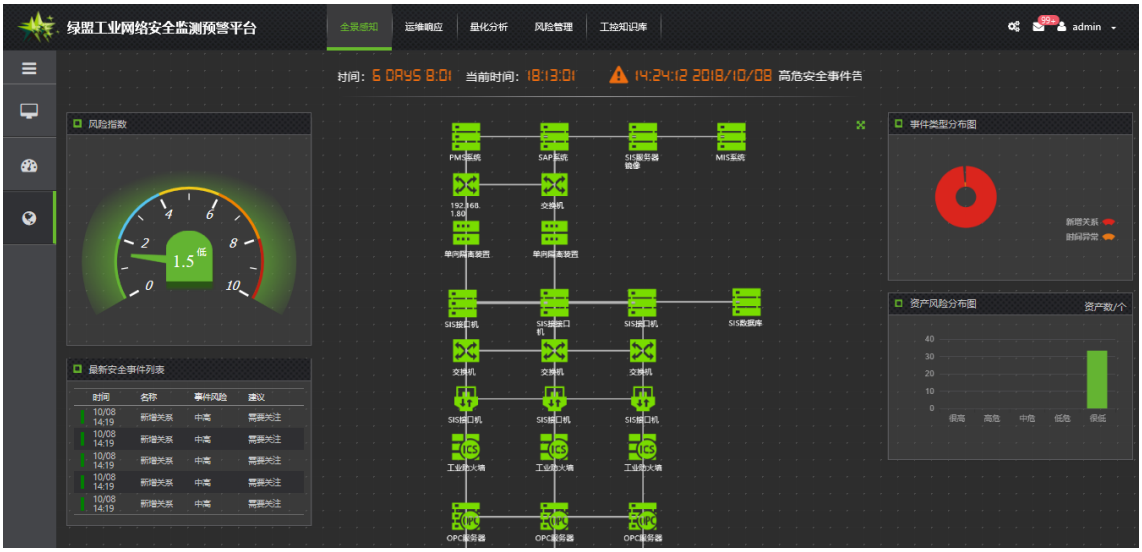


图 2.4 工控网络综合态势管理和场景拓扑定制

一站式的信息综合管理

工业网络安全监测预警平台提供一站式的信息综合管理功能。一站式综合管理包括对安全设备上传的事件类日志信息、业务系统上传的操作等日志信息、采集的安全设备配置策略信息进行统一的分析和呈现。

日志管理功能模块支持上位机服务器、数据库服务器、工业网络通信设备的日志采集和接入。采集服务器、工作站的用户登录、操作信息、运行状态、移动存储设备接入、网络外联等事件信息；采集数据库的操作信息、运行状态等事件信息；采集网络设备的用户登录、操作信息、配置信息变更、流量信息、网口状态等信息。

一站式信息综合管理如图。

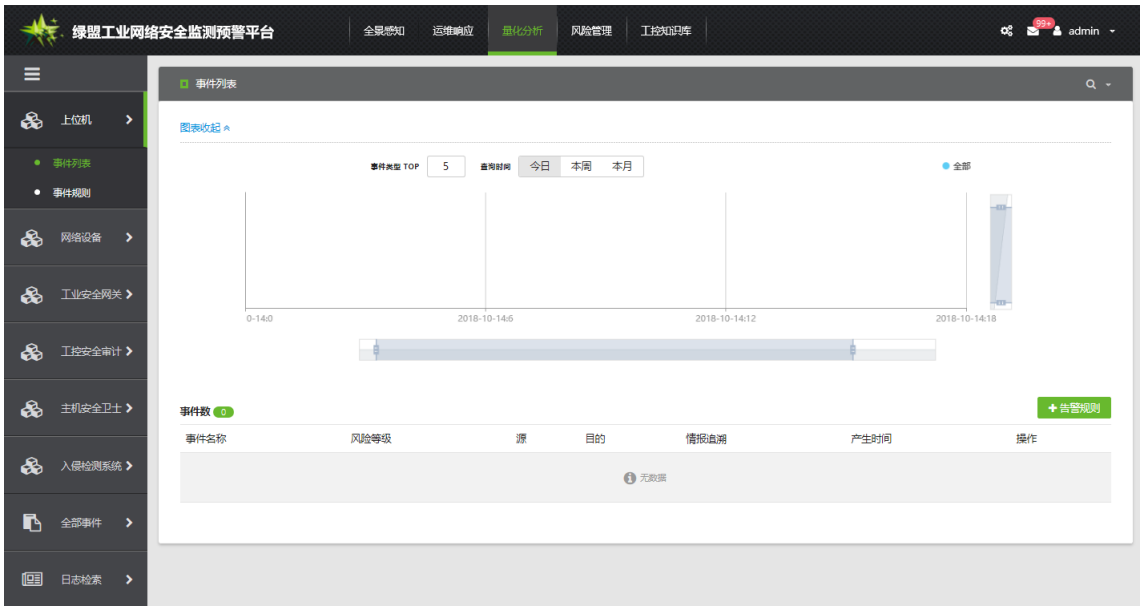


图 2.5 一站式综合信息管理

工控安全设备管理

目前，INSP 设备管理功能模块支持工业安全网关、工控安全审计系统、工控漏洞扫描系统等设备接入。统一监控绿盟工控安全设备，对设备网络配置、路由配置、DNS 配置、系统服务、升级策略和配置备份等进行配置，实现设备配置基线管理。

© 2019 绿盟科技

密级：完全公开

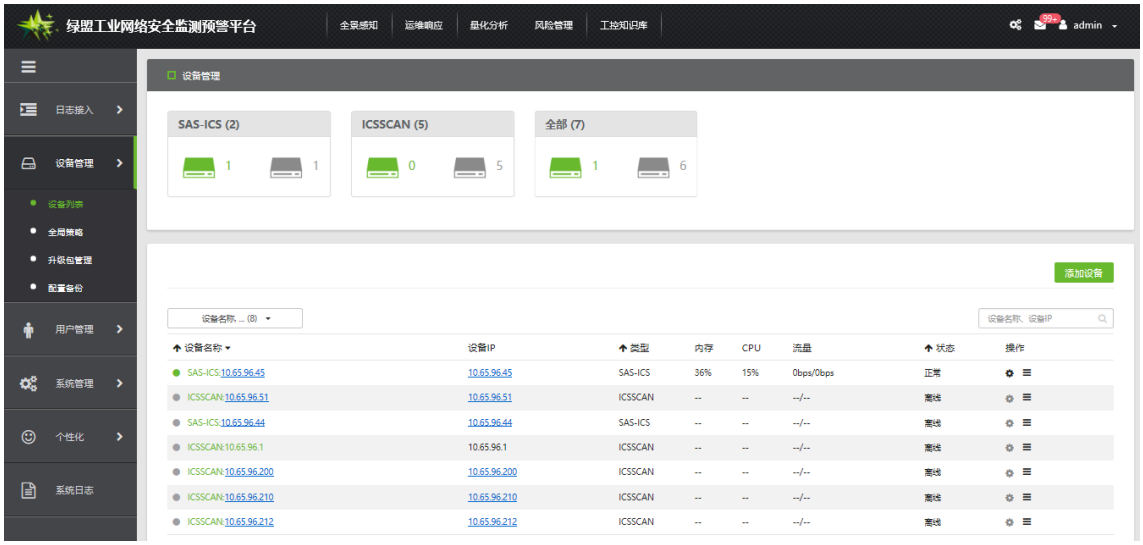


图 2.6 工控安全设备管理

融合业务特性的工控知识库

工业网络安全监测预警平台基于多类型的工控知识库进行事件的关联分析。深入到不同行业的工控网络特性当中，产生融合业务特点的场景告警。同时又具备工业网络全行业属性的通用性告警，如针对资产新增、路径异常、未知协议、越权操作、关键控制等操作产生的告警。

工控知识库包括工控事件库、处置预案库、工控漏洞库、工控协议库。平台主要依据工控事件库和处置预案库将多种设备收集的日志进行整合关联分析，产生告警并给出处置建议。

工控漏洞库包含了 IT 信息系统漏洞及 OT 工控环境漏洞，方便运维人员进行风险分析和管控。

工控协议库囊括了 Modbus Tcp、S7、S7 PLUS、Profinet、DNP3、IEC 60870-5-104、IEC 61850-MMS 等主流工控厂商使用的工控通信协议。

通过工控知识库的建立可以达到强大的关联分析效果。比如平台从生产控制网络的资产行为中建立了一组正常行为基线，即到一组 PLC 的 Modbus 所有通信都是来自于相同的 3 个 HMI 工作站，标记为基线 A。在运营过程中发现监控系统报警，与基线 A 出现分歧，出现了第 4 个系统与 PLC 进行通信，判断其可能的表现有四种：一个新的未被授权的设备被插入网络中（如一台管理员的笔记本电脑）；一个使用欺诈 IP 地址的恶意 HMI 正在运行；新

© 2019 绿盟科技

密级：完全公开

的系统安装上线。通过对近期公网的威胁情报及生产控制网络近期操作行为的整合分析，得知该异常是由于未被授权的设备接入网络所导致。

高级威胁分析

- APT 是一种高级持续性威胁，通过长期潜伏找到有价值的特定目标，利用网络中受信的应用程序漏洞，发起持续性网络攻击，窃取核心资料或篡改数据。但任何攻击行为都会有他的行为特点，如嗅探，提权，安装后门，扩散和逃逸等行为。绿盟根据多年工程经验结合美国 NASA 的攻击链条模型设计出针对攻击行为特征的安全分析模型，通过该模型，用户不必具有很高的专业安全能力就可以准确的对安全事件进行发现，预测和历史痕迹追踪，从而降低对专业安全分析人员的要求，减轻企业成本。

关键技术

工业网络数据采集

NSFOCUS INSP 可以支持代理日志采集方式和多种标准协议。通过数据采集、数据理解、数据抽取和数据清洗等操作，将各种应用系统和设备的日志进行预处理，帮助管理员把工业网络日志进行去噪，提取其中人们事先不知道，但有潜在有用的信息和知识。

独家数据强化技术

NSFOCUS INSP 根据绿盟科技对攻防研究的长期积累，提供一套简洁有效的日志统一分类，使用独有的技术将日志快速标准化，并基于安全分析需要进行数据的过滤和强化，丢弃无法用的噪音信息，提升日志查询和分析效率。

© 2019 绿盟科技

密级：完全公开

强大的分析引擎

平台中预制关联分析引擎，预制引擎构成分析平台的核心功能并且对专项分析提供基础能力，如风险分析、脆弱性分析、态势分析、资产分析、攻击链条分析等。

分析引擎采用分布式设计能够进行横向扩展，面临工业网络数据量时能够实现按需扩展，将分析引擎分散到其他更多的机器中，实现按需进行计算资源扩展。

面向业务的插件化设计

NSFOCUS INSP 采用全新大数据框架，将上层业务模块插件化处理，使业务模块与平台功能进行一对一设计，业务模块的改善和增加就不会造成其他模块或平台功能的调整，也就是将业务模块抽象并与平台功能实现分离，从而提高研发效率，降低企业维护成本。

可靠性

NSFOCUS INSP 采用大数据组件，对数据对象弹性分布存储 3 个存储节点中，并采用线程级监控，一旦发现问题，可迅速恢复并告警，同时 3 备份可以提供完整的灾难恢复功能。

多地部署

针对大型多组织的企业和机构，采集器可以部署在异地站点或二级单位（保持网络可达），分析中心部署在总部节点，异地站点将采集到的数据定时通过 FTP 或 SFTP 上传到上级分析中心，供本地留存和查询服务。

产品功能

© 2019 绿盟科技

密级：完全公开

功能	描述
全景视图	支持大屏投放要求及分辨率兼容要求，易于操作。展现形式多样，画面丰富，并且能够多种图形化方式展现网络安全态势情况，动态提醒当前网络最新的安全威胁。
工控安全设备管理	INSP 设备管理功能模块支持工业安全网关、工控安全审计系统、工控漏洞扫描系统等设备接入。统一监控绿盟工控安全设备，对设备网络配置、路由配置、DNS 配置、系统服务、升级策略和配置备份等进行配置，实现设备配置基线管理。
工业网络综合态势管理和场景拓扑定制	工业网络安全监测预警平台可以通过网络拓扑或直观呈现的方式表现网络环境及各设备的运行状态和安全状态，从而达到对工控网络中的各类设备进行集中的状态及性能监控的目的。目前主要通过定制化工控拓扑的方式来实现工控网络综合态势的管理和呈现。呈现在首页的工控网络拓扑可根据工业现场需求进行定制化的拓扑绘制。

© 2019 绿盟科技

密级：完全公开

资产管理	NSFOCUS INSP 建立了一套完整的多维度资产管理系统，支持从资产维度对工业企业网络内部的存在的威胁进行统计和分析。帮助运维人员洞悉企业内部 IT 基础设施的情况，包括：资产 IP 地址、名称、开放的协议端口和应用。
风险管理	NSFOCUS INSP 提供以资产为视角的漏洞治理功能。 支持对脆弱性、漏洞、工业网络安全事件、资产等数据进行统计分析汇总，以各类统计图表方式，围绕资产，呈现风险、漏洞及工业网络安全事件数量及变化趋势等，支持对漏洞操作处理，添加解决方案。
工作台	工作台是整个系统的运维入口，系统中绝大多数运维功能都能从这里进入。并且，在本页面中，为用户呈现了各业务基本的统计信息；以及预警列表快捷展示。
报表管理	系统内置了资产、事件、监控等报表报告，用户可以预览查阅。报表报告的产生都能够调度、定期自动生成。系统内置报表编辑器，用户可以自定义报表
工控知识库	工控知识库包括审计规则、工控漏洞库、工控协议库。平台主要依据工控漏洞库和处置预案库将多种设备收集的日志进行整合关联分析，产生告警并给出处置建议。工控漏洞库包含了 IT 信息系统漏洞及 OT 工控环境漏洞，方便运维人员进行风险分析和管控。工控协议库囊括

© 2019 绿盟科技

密级：完全公开

	了 Modbus Tcp、S7、S7 PLUS、Profinet、DNP3、IEC 60870-5-104、IEC 61850-MMS 等主流工控厂商使用的工控通信协议。
权限管理	NSFOCUS INSP 不仅提供三权分立的设计，内置系统管理员、业务管理员和审计管理员。还能够基于角色的权限管理机制，对所有用户的权限通过角色来分配
系统管理	系统具有丰富的自身配置管理功能，包括自身配置、系统运行参数监控等。系统具有自身运行监控与告警、系统日志记录，存储，备份等功能。

三. 典型部署

部署方式

单级部署

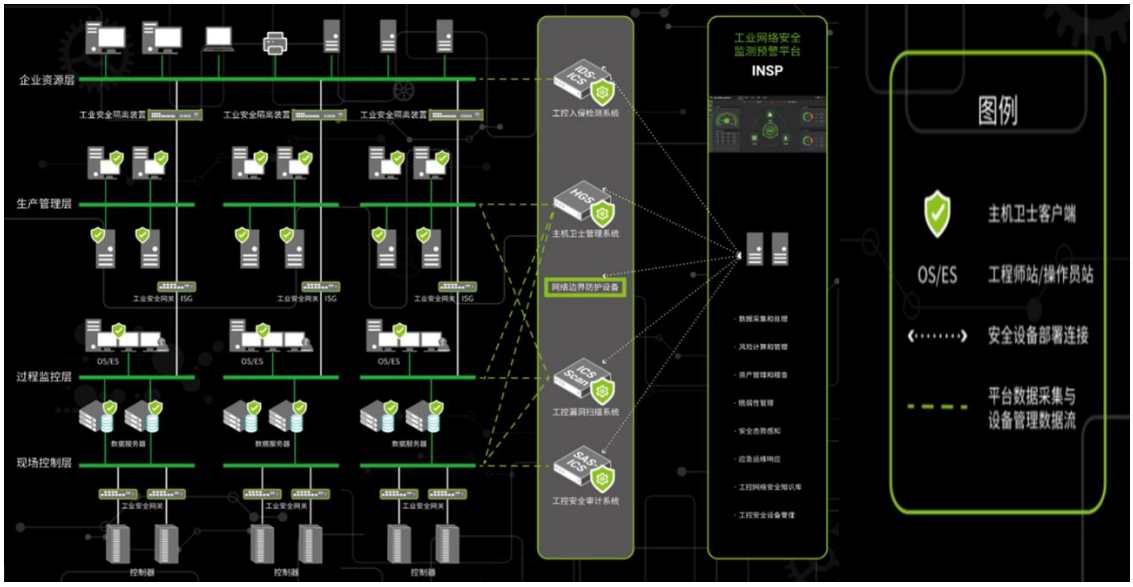
在工业网络中就部署一个管理中心程序，所有的用户都登录到该管理中心进行访问，通过系统权限设置来区分不同的管理职责。

在单级部署模式下，又分为单机部署和集群部署。

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分企业客户的工业网络环境。在单机部署场景中，用户仅需在一台服务器上部署 NSFOCUS INSP 系统。之后，管理中心可以收集设备对象的日志和性能信息。用户可以通过浏览器登录系统的交互界面，并根据相应的权限进行各种管理操作。

© 2019 绿盟科技

密级：完全公开



单级部署模式

多级部署

多级部署是指将 INSP 采用多地，按照分组的运行的方式进行部署的模式。一般地，当需要在分散在工业企业网络中进行较大规模的节点部署时，此时，大量的性能、日志数据通过网络汇总到集团管理中心，会给管理中心造成一定的性能影响。通过在将 NSFOCUS INSP 平台运行于工业企业集团不同数据管理中心的方式，上至业务层网络，下达生产现场，实现集团对工业生产网络安全的全局把控。提供从工业网络安全评估到事件响应在内的全周期安全服务。

© 2019 绿盟科技

密级：完全公开

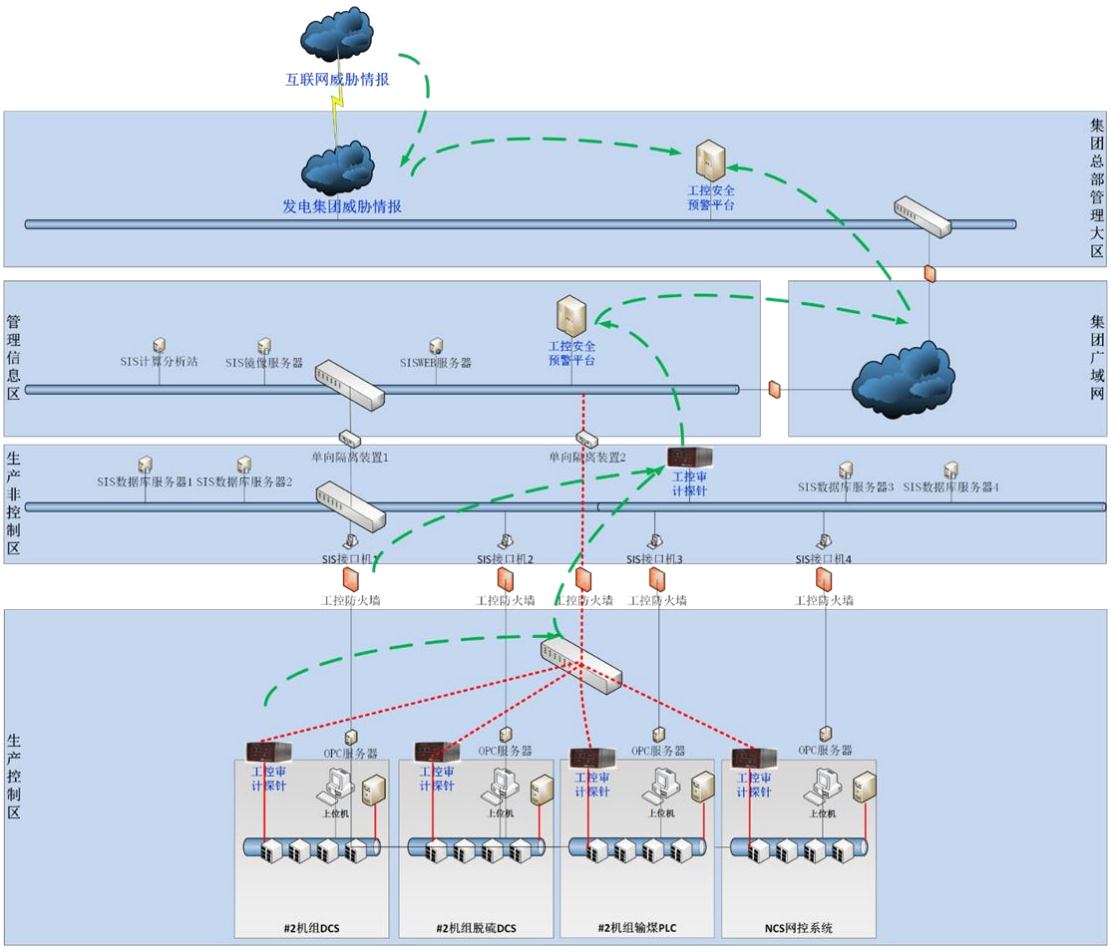


图 3.1 多级部署模式

运行环境

NSFOCUS INSP 的运行环境：

主机硬件配置要求

硬件	服务器（I）	服务器（II）
CPU	2*E5-2630V2（6 核心 12 线程、2.6GHz）	2*E5-2630V2 （6 核心 12 线程、2.6GHz）
内存	64GB DDR 3 1333MHz	128GB DDR 3 1333MHz
硬盘	8*1TB（ext4 文件系统格式、7200 转），Raid5	8*1TB（ext4 文件系统格式、7200 转），Raid5
网卡	千兆网卡	千兆网卡
Raid 卡	带缓存 raid 卡，推荐 PERC H710p	带缓存 raid 卡，推荐 PERC H710p

© 2019 绿盟科技

密级：完全公开

硬件	服务器（I）	服务器（II）
光驱	内置光驱	内置光驱
电源	热插拔冗余电源（1+1）1100 瓦	热插拔冗余电源（1+1）1100 瓦

注意：详细要求参见产品部署指南

主机软件配置要求

软件	要求
操作系统	目前只支持 64 位操作系统，要求安装时关闭 SELinux。 • CentOS 6.5 x86_64，basic server 模式。 • CentOS 7.3 x86_64，infrastructure server 模式。

注意	硬盘可用空间主要指/opt 目录所在挂载分区的可用磁盘空间。 为了方便维护，建议所有节点安装相同类型的操作系统。 集群节点间为千兆网络环境。

客户端环境要求：

用户通过浏览器即可访问管理中心。系统推荐使用微软 IE11，Google Chrome 或者 Mozilla Firefox 最新版本浏览器。浏览器所在 PC 的内存推荐 4GB。

四. 结论

由于工业控制系统所覆盖的行业重要性，比如油化、电力、核电厂、水利、交通、市政、军事、高端制造业等，其安全性问题也越发的重要，并且牵涉到国计民生。对于这些关键信息基础设施，如何进行安全监测及预警，如何及时有效的进行事前的防范，事中的监测以及事后的追溯，正成为工控安全领域亟待解决的问题。

基于全生命周期的工控系统安全综合保障手段的建设，给传统的单点安全防护提供了新的思路。将功能安全、信息安全进行深度融合的工业网络安全监测预警平台，连接了孤军奋战的单个结点，融入了故障诊断、异常告警、态势感知、攻击检测等持续可运营的安全防护理念，最大限度的保障工业控制系统稳定、高效、安全的运行。

© 2019 绿盟科技

密级：完全公开